

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Sub B
Claim 1 (original): A method for filtering packets, comprising:
receiving a packet sent from a first device to a second device;
authenticating an identifier for said packet;
determining whether to send said packet to said second device; and
sending said packet to said second device in accordance with said determination.

AI
Claim 2 (original): The method of claim 1, wherein said determining comprises:
comparing said identifier to a list of identifiers;
retrieving at least one policy rule;
determining whether to send said packet to said second device in accordance with said comparison and said policy rule.

Claim 3 (original): The method of claim 1, wherein said identifier is a common host identifier.

Sub B
Claim 4 (original): The method of claim 1, wherein said authenticating is performed in accordance with IPSEC standards.

Claim 5 (original): The method of claim 1, wherein said authenticating comprises:
retrieving a pointer to a security association from an authentication header from said packet;
retrieving a key associated with said security association; and
determining whether said packet is authentic using said key.

Claim 6 (original): The method of claim 5, wherein said identifier is not authentic, further comprising sending a first message to a third device indicating said identifier is not authentic.

Claim 7 (original): The method of claim 5 wherein said authentication header is an IPSEC authentication header.

Claim 8 (original): The method of claim 1, wherein said packet is encrypted prior to said receiving, further comprising decrypting said packet prior to authenticating.

Claim 9 (original): The method of claim 8, wherein said packet is encrypted and decrypted using one of group of cryptographic techniques comprising DES, triple DES, HMAC and RSA.

~~Claim 10 (original): The method of claim 1, wherein said policy rule is stored in a policy configuration file at said second device.~~

Claim 11 (original): A machine-readable memory whose contents cause a computer system to perform packet filtering, by performing the steps of:
receiving a packet sent from a first device to a second device;
authenticating an identifier for said packet;
determining whether to send said packet to said second device; and
sending said packet to said second device in accordance with said determination.

Claim 12 (original): The machine-readable memory of claim 11, wherein said determining comprises:
comparing said identifier to a list of identifiers;
retrieving at least one policy rule;
determining whether to send said packet to said second device in accordance with said comparison and said policy rule.

Claim 13 (original): The machine-readable memory of claim 11, wherein said identifier is a common host identifier.


~~Claim 14 (original): The machine-readable memory of claim 11, wherein said authenticating is performed in accordance with IPSEC standards.~~

Claim 15 (original): The machine-readable memory of claim 11, wherein said authenticating comprises:

retrieving a pointer to a security association from an authentication header from said packet;

retrieving a key associated with said security association; and
determining whether said packet is authentic using said key.

Claim 16 (original): The machine-readable memory of claim 15, wherein said identifier is not authentic, further comprising sending a first message to a third device indicating said identifier is not authentic.

 Claim 17 (original): The machine-readable memory of claim 15 wherein said authentication header is an IPSEC authentication header.

Claim 18 (original): The machine-readable memory of claim 11, wherein said packet is encrypted prior to said receiving, further comprising decrypting said packet prior to authenticating.

Claim 19 (original): The machine-readable memory of claim 18, wherein said packet is encrypted and decrypted using one of group of cryptographic techniques comprising DES, triple DES, HMAC and RSA.

Claim 20 (original): The machine-readable memory of claim 11, wherein said policy rule is stored in a policy configuration file at said second device.

Claim 21 (original): A packet filter for a distributed firewall, comprising:
an input means coupled to said first network for receiving a data packet from a first device, said data packet having an encrypted common host identifier;
a first buffer coupled to said input means for storing said received packet;
a first memory segment containing a list of common host identifiers and at least one policy rule;

a second memory segment for storing a program for decrypting said common host identifier, authenticating said common host identifier, and determining whether to send said packet to a second device based on said list and said policy rule;

a processor coupled to said first buffer, said first memory segment and said second memory segment for executing said program; and

an output means coupled to said first buffer for forwarding said compared data packet to said second device based on said comparison.

Claim 22 (currently amended): The apparatus of claim 21, further comprising a second buffer for storing said compared data packet prior to forwarding said compared data packet to the second device.

Claims 23-28 (cancelled).

Sub B1
Claim 29 (original): A distributed firewall system, comprising:
a first network device;
a second network device in communication with said first network device;
a packet filter processor for each network device;
an encryption means coupled to said packet filter processor, said encryption means for decrypting and authenticating a packet sent between said first network device and said second network device; and
a system management module to manage said packet filter processors.

Sub B2
Claim 30 (new): The system of claim 29 wherein said authenticating comprises:
retrieving a pointer to a security association from an authentication header from said packet;
retrieving a key associated with said security association; and
determining whether said packet is authentic using said key.

Claim 31 (new): The system of claim 30 wherein said authentication header is an IPSEC authentication header.